

Claims

sub B1

1. A method for copying a program having a scrambled program content component and an encrypted control component comprising:
- 5 (a) receiving, in a recording apparatus, said program;
- (b) attaching a data item to said encrypted control component, said data item indicating that said program has been copied;
- (c) encrypting said encrypted control component and said data item to generate a nested control component; and
- 10 (d) recording said program content component and said nested control component.
2. The method of Claim 1 wherein the steps of receiving, attaching and encrypting are performed in a smart card coupled to said recording apparatus.
- 15 3. The method of Claim 2 wherein said encrypted control component comprises copy control information, a descrambling key associated with said scrambled program content component.
- 20 4. The method of Claim 3 wherein said copy control information indicates one of never-copy state and copy-once state.
5. The method of Claim 4 wherein said encrypted control component is encrypted using a global public key.
- 25 6. The method of Claim 5 wherein said nested control component is encrypted using said global public key.

7. The method of Claim 6 wherein said global public key is associated with said smart card, said smart card having a corresponding private key stored therein.

5 8. The method of Claim 7 wherein said encrypted control component further comprises purchase information comprising channel identification data, event identity data, date and time stamp data, and billing data.

10 9. The method of Claim 8 wherein said smart card comprises a card body with a plurality of terminals arranged on a surface of said card body in accordance with one of ISO 7816 and PCMCIA card standards.

10. The method of Claim 9 wherein said recording apparatus is a digital video cassette recorder.

15 11. The method of Claim 10 wherein said recording apparatus is a recordable DVD apparatus.

20 12. A method for managing access to a copy of a restricted program, said method comprising:

- 25 (a) receiving said restricted program in a processing apparatus, said restricted program having a scrambled program content component and a nested control component, said nested control component being encrypted;
- (b) decrypting said nested control component to obtain an encrypted control component and a data item, said data item indicating that said restricted program has been copied;
- (c) decrypting said encrypted control component to obtain a descrambling key and copy control information;

- 5
- (d) comparing said copy control information and said data item to determine if said copy is valid; and
 - (e) descrambling said program content component, using said descrambling key in response to a determination that said copy is valid.
- 10
13. The method of Claim 12 wherein said encrypted control component and said nested control component are encrypted using a global public key.
14. The method of Claim 13 wherein the steps of receiving, decrypting, comparing and descrambling are performed in a smart card coupled to said processing apparatus, said steps of decrypting employ a private key stored in said smart card and associated with said global public key.
- 15
15. The method of Claim 14 wherein said encrypted control component further comprises purchase information comprising channel identification data, event identity data, date and time stamp data, and billing data.
- 20
16. The method of Claim 15 wherein said purchase information comprises the cost of said program, said method further comprising:
- (a) deducting the cost of said program from a cash reserve stored in said smart card to determine a calculated cash reserve;
 - (b) descrambling, in said smart card, said scrambled program content component using said descrambling key in response to having a positive calculated cash reserve; and
 - (c) passing said descrambled transmitted event to said video processing apparatus.
- 25
17. The method of Claim 16 wherein said cash reserve is downloaded in an e-cash certificate message from an automatic teller machine.
- 30

18. The method of Claim 17 wherein said processing apparatus is one of a digital video cassette recorder/player and a DVD recorder/player.
- 5 19. The method of Claim 18 wherein said smart card comprises a card body with a plurality of terminals arranged on a surface of said card body in accordance with one of ISO 7816 and PCMCIA card standards.
- 10 20. A method for managing access to a recorded copy of a restricted program using a smart card coupled to a video processing apparatus comprises:
- (a) transferring, from a bank, a cash reserve to said smart card;
 - (b) receiving, in said smart card, said recorded copy of said restricted program from said video processing apparatus, said restricted program having a scrambled audio/video component and a nested control component, said nested control component being encrypted;
 - 15 (c) decrypting said nested control component to obtain an encrypted control component and a data item, said data item indicating that said restricted program has been copied;
 - (d) decrypting said encrypted control component to obtain a
 - 20 descrambling key, copy control information and purchase information;
 - (e) comparing said copy control information and said data item to determine if said copy is valid;
 - (f) verifying that the cost of said restricted program is less than the
 - 25 stored cash reserve and deducting the cost of said restricted program from said stored cash reserve;
 - (g) descrambling said audio/video component, using said descrambling key.

